# Report Says Election Offices ‘Highly Susceptible’ to Digital Attacks. What Now?

It's an easy fix.

Amanda Ziadeh

Sun, 08/26/2018 - 10:25

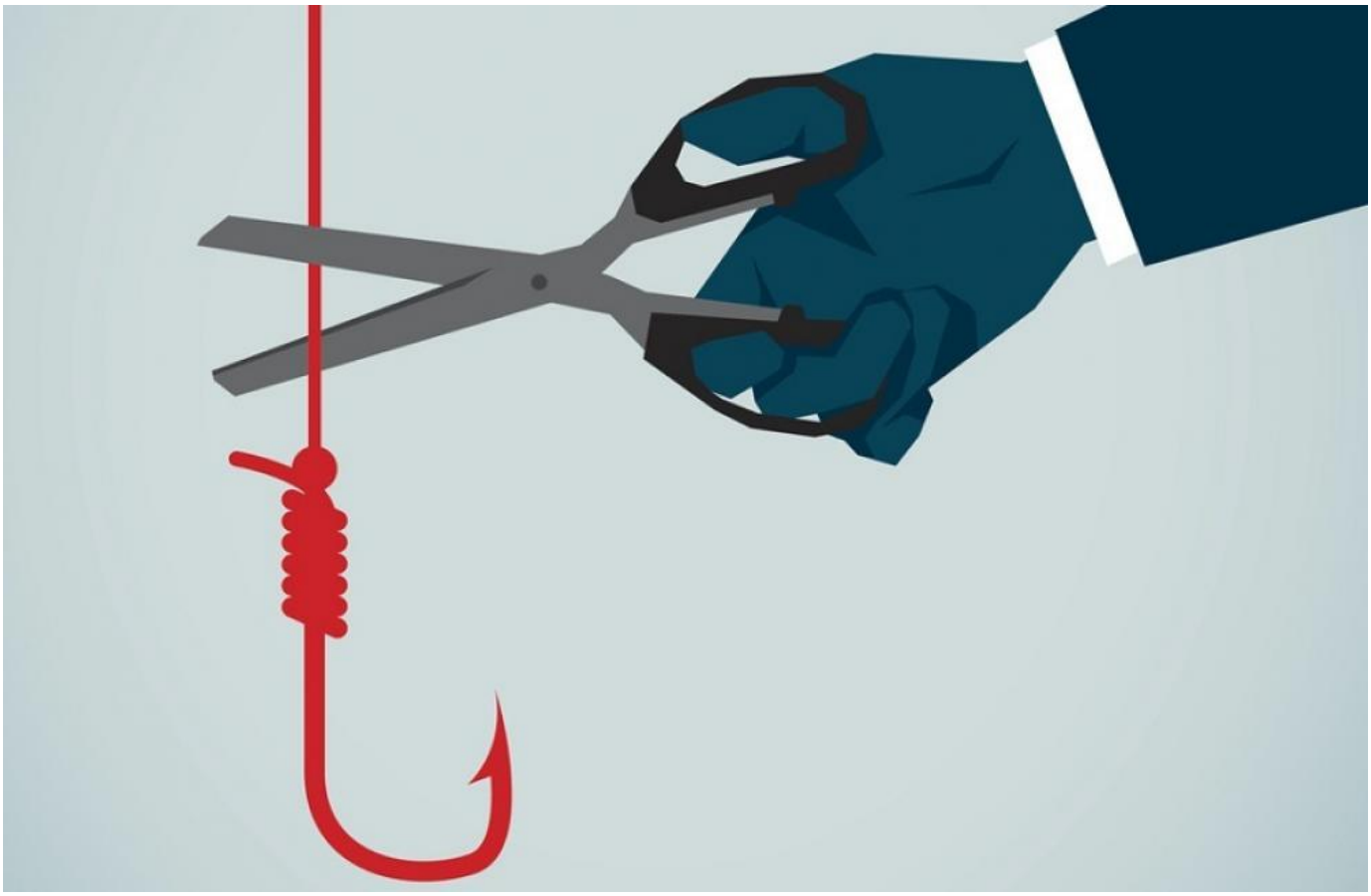

Illustration: erhui1979/iStock

Despite warnings about possible cyberattacks aimed at undermining midterm election security, new research reveals an overwhelming number of evaluated state, territory and District of Columbia election offices as highly vulnerable to email spoofing.

Released today, the “Email Spoofing Threat to the 2018 U.S. Midterm Elections” report by Anomali Labs, the R&D arm of threat intelligence company Anomali, explores the strength of email security programs for election-related infrastructure. And of the 90 state, territory and District of Columbia election offices Anomali Labs

assessed, 96 percent are “highly susceptible” to email spoofing attacks

The report found a low adoption rate of strong email authentication and email security standards among the majority of state-level election offices and their online voter registration sites. Adoption overall is inconsistent across the board. Being spoofable means threat actors could falsify the sender’s origins to appear as if the fraudulent email came from a legitimate government organization, according to the report.

This type of threat is “100 percent real, and as far as urgency, given that phishing is the No. 1 attack vector, not just against election officials but also in industry in general, I think it’s very, very high,” said Roberto Sanchez, Anomali director of threat and sharing analysis and the lead researcher for the election security report.

And the email spoofing attacks on election systems do happen. A recent one occurred before the 2016 presidential election when Russian state-sponsored actors targeted the American Samoa Election Office by sending test emails to addresses at the office to see if those accounts were active, in order to potentially launch a phishing attack, The Intercept reported.

And, of course, the Russian government compromised the emails of U.S. political organizations associated with the 2016 U.S. presidential elections and exposed those hacked emails on DCLeaks.com and WikiLeaks, according to a joint statement by the FBI and Homeland Security Department.

“It’s a known tactic and it’s extremely easy to fix, so that’s why we want to make sure that it’s pressed upon the local and state that they are empowered to protect themselves with quick measures,” Sanchez said.

These email security standards are easy to implement, and there are many that help detect and fight off email forgery, he added. In fact, “it’s as simple as, I could probably do it overnight for all the states and territories myself,” Sanchez said, and developing the policies is especially uncomplicated.

## Report Results

Anomali Labs researchers looked at three email authentication protocols: one DNS resolution security control, and two secure mail server controls to find the states and territories susceptible to email spoofing attacks, eavesdropping and traffic

redirection.

A DNS server holds a directory of domain names and translates them into internet protocol addresses. The report found none of the evaluated domains published DNS-based Authentication of Named Entities records, which certify encryption for special domains. Publishing these records helps ward off active threat actors from removing a certain email protocol command that tells an email server an email client wants to turn an existing insecure connection to a secure one, so an attacker can manipulate mail traffic.

The report also found there's a low adoption rate across the 50 states, D.C., and five U.S. territories for email authentication controls. Only 34 percent publish Sender Policy Framework records, 10 percent implement DomainKeys Identified Mail records and 15.5 percent deploy Domain-based Message Authentication, Reporting and Conformance records.

SPFs specify the hosts authorized to send email on behalf of the domain; DKIMs prove an email came from the right sender and that nothing was changed on its way; and DMARCs provide the policies for how to handle failures in SPF or DKIM. So, these protocols are pretty important.

And finally, just 12 percent of the evaluated domains use a digital signature tool that allows servers to authenticate the integrity of DNS responses to queries, proving they haven't been spoofed.

Sanchez said he didn't find any active phishing against candidates or localities, but there were spam emails that came out of a number states, and theoretically, that means those states can be spoofed. But seeing evidence of spam wasn't surprising, because the email systems were "wide open."

## Further-facing Implications

These threats the midterm elections face this November could bleed into the next presidential election if localities aren't careful.

"Even if we're electing either a mayor to a congressional person to a president, all of those votes that are tabulated by the electorate are all done at the local and state level," Sanchez said. "If these issues aren't corrected, then it's just another additional vector allowed, presenting an opportunity for a nation-state actor to

exploit.”

And it doesn’t necessarily have to be a nation-state actor; a  low-level hacker can use the same exploits. But nation-state actors have the resources, motivation and sophistication to do more harm, to craft a more convincing message.

## What Should be Done

If these security measures are so easy to implement, why aren’t local, state and tribal territories using them?

According to Sanchez and based off his experience as an information security practitioner, it comes down to resource constraints and talent, meaning election office staff isn’t knowledgeable or aware this is an issue and how simple it is to fix.

The report also included recommendations, starting with publishing all the proper SPF, DKIM, DMARC and other email security and certificates with strict policies on all domains and mail servers.

For good measure, Anomali Labs also recommends testing mail server configurations against the enterprise policy to find any weakness and fix any issues, and educate users on basic security awareness and how to spot fraudulent emails.

And Sanchez said the federal government can help by continuously providing recommended actions, security and operational directives on how to secure email and web security, and proactively pushing them out to the local and state levels so they can coordinate with their respective agencies.

Local, state and tribal territorial governments should take advantage of free or low-cost sources, including the Multi-State Information Sharing and Analysis Center, the Elections Infrastructure ISAC and the DHS, Sanchez added.

## Takeaway

So, should the public worry about the election machines, systems, hardware and software being disrupted at a massive scale?

The answer is no, because the election infrastructure is decentralized and every state’s voting system isn’t connected to the next, Sanchez said. It’s unlikely  a state-

sponsored actor has the resources to hit all 50 at once.

But Sanchez had a final word of caution.

“Where I think that we should be concerned about as a society as a whole is more disinformation, the sewing of discourse, pitting left versus right,” he said. “That’s more of a threat to us than any manipulation of any voting systems.”

View printer friendly version
phishing
nation state actors
Anomali Labs
email security
email spoofing
election
election security
Department of Homeland Security
data protection